Belief Logics: BAN

The BAN (Burrows, Abadi, and Needham) logic is a modal logic of belief. It has several modal operators including:

- \( P \models X \): (P believes X) P is entitled to act as though X is true.
- \( A \triangleleft X \): (A sees X) someone has sent a message to A containing X so that he can read X and repeat it.
- \( A \models \sim K \): (A once said K) at some time, A used key K.
- \( A \models \sim X \): (A once said X) at some time, A uttered a message containing X.
- \( A \implies X \): (A has jurisdiction over X) A is an authority on X and can be trusted on X.
- \( A \leftrightarrow B \): (A and B share key K) A and B can use key K to communicate. The key is unknown to anyone else.

BAN Operators Continued

- \( #(X) \): (X is fresh) meaning that X has not been sent before in any run of the protocol.
- \( K \rightarrow B \): (B has public key K) B has a published public key K and corresponding private key \( K^{-1} \).
- \( A \leftrightarrow X B \): (A and B share secret X) X is a secret known only to A, B and possibly some trusted associates.

Belief Logics: Rules

There are numerous rules of inference for manipulating the protocol to generate a set of beliefs. For example,

Message meaning: If A believes (A share(K) B) and A sees \( \{X\}_K \) then A believes (B said X).

\[
A \models (A \leftrightarrow K B), A \triangleleft \{X\}_K \\
A \models (B \sim X)
\]
**Belief Logics: Rules**

**Nonce verification:** If A believes X is fresh and A believes B once said X, then A believes B believes X.

\[
A \models (\#(X)), A \models (B \models \neg X) \\
\frac{}{A \models (B \models X)}
\]

**Jurisdiction:** If A believes B has jurisdiction over X and A believes B believes X, then A believes X.

\[
A \models (B \models X), A \models (B \models X) \\
\frac{}{A \models X}
\]

**BAN Logic: Idealization**

To get from protocol steps to logical inferences, we have a process called *idealization*. This attempts to turn the message sent into its intended semantics. For example, given the protocol step:

\[
A \to B : \{A, K_{ab}\} \leftarrow \{K_{bs}\}
\]

If B knows the key \(K_{bs}\), this tells us that \(K_{ab}\) is a key to communicate with A. An idealized version is:

\[
A \to B : \{A, K_{ab}\} \leftarrow \{K_{bs}\}
\]

One purpose of idealization is to omit parts of the message that do not contribute to the beliefs of the recipients. *In BAN all plaintext is omitted since it can be forged.*

Idealization of the protocol is not defined unambiguously. It depends on the interpretation of the meaning of some steps.

**Lessons**

- The BAN logic has been an important tool for reasoning about protocols.
- It is a modal logic of belief with 10 primitives and a number of inference rules.

**Next lecture:** The BAN Logic: Needham-Schroeder